REMARKS

As a preliminary matter, Applicant notes that claim 36 has been amended to correct a minor typographical error not noted by the Examiner. No new matter has been added.

Turning now to the rejections, the present invention is directed to a system that provides security for a protected function. In one embodiment, a wireless communications device stores an authorization code in memory. The authorization code may be provided by a central controller, and is based on a master code stored at the central controller. To gain access to a protected function (e.g., unlocking a locked door), the wireless communications device transmits an access request to an access control device associated with the door (e.g., a door lock). The access control device responds by transmitting an authentication challenge to the wireless communications device. Based on both the authentication challenge and the authentication code stored in memory, the wireless communications device computes an authentication response and returns the response to the access control device. If the access control device recognizes the authentication response as valid, the user gains access to the protected function (e.g., the door is unlocked).

The Examiner rejected claim 1 under 35 U.S.C. §103(a) as being unpatentable over Henderson. Claim 1 recites that the wireless communications device "[receives] an authentication challenge from said access control device ... [and computes] an authentication response based on said authentication challenge and said authorization code." The Examiner contends that, although Henderson does not teach or suggest authentication, it would have been obvious to modify the disclosed system to use authentication since authentication is known. Applicant disagrees.

Henderson discloses a system and method by which users may gain access to real estate lock boxes. The system of Henderson includes a lockbox, a key, and a stand to provide the key and the lockbox with a variety of data. According to Henderson, the lockbox and the key operate responsive to the exchange of signals between the two. However, the signal

transmitted from the lockbox to the key only provides the key with certain information (i.e., the condition of the lockbox battery and the date). As the Examiner readily admits, an authentication challenge is not part of the signal. By definition, the key of Henderson cannot compute an authentication response based on an authentication challenge it never receives. Even if one could consider the transmitted signal as an authentication challenge (which it cannot), the response provided by the key contains only data that is already stored in the key's memory (i.e., pre-programmed into the key by the stand). The key does not include the data received in the signal in the response. *E.g., Henderson*, col. 23, ln. 64 – col. 24, ln. 31. Henderson never teaches or even suggests that the key computes the content of the response based in part on the data in the received signal. As such, Henderson does not teach or suggest claim 1 and the §103 rejection fails.

The Examiner also rejected claims 15, 40, and 60 under 35 U.S.C. §103(a) as being unpatentable over Henderson for the same reasons as those cited above for claim 1. Claim 40, however, is directed to a device that comprises "a processor to compute to compute said authentication response based on said authentication challenge received from said access control device and said authorization code." Claims 15 and 60 are directed to the access control device that receive the authentication response, but recite that the authentication response is based on the authentication challenge and an authorization code stored in memory of the wireless communications device. Therefore, for reasons similar to those stated above, Henderson also fails to teach or suggest any of claims 15, 40, and 60.

The Examiner also rejected claim 36 under 35 U.S.C. §103(a) as being unpatentable over Wang. Claim 36 is directed to a central controller that computes the authentication code for the wireless communications device responsive to an initialization request received from the wireless communications device. The Examiner admits that Wang does not teach or suggest "initialization" as recited in claim 36. While this is true, there is an even more glaring deviation.

Notably, Wang does not teach or suggest a central controller that "[computes] an authorization code based on [a] master code ... in response to receipt of [an] initialization request."

Wang discloses a system that is used in Point-Of-Sale (POS) operations. In Wang, a server may transmit a transaction program (TP) to a user's Portable Electronic Authorization Device (PEAD). The TP includes an executable portion that may comprise sets of codes. Far from being an authorization code, however, these codes are used by the PEAD to encrypt data that approves a POS transaction. *Wang*, col. 3, ll. 24-32. Additionally, the codes may be used to search a user's computing device for the PEAD (i.e., to detect the presence of the PEAD), or to query for and retrieve user identification information from the user's device. *Wang*, col. 16, ll. 7-33. Wang does not teach or suggest that a central controller computes an authorization code for the user based on a master code. Nor does Wang teach or suggest that the device receives an authorization code. In fact, Wang does not teach or suggest that the server even has a master code. As such, Wang fails to teach or suggest claim 36.

The Examiner also rejected claim 72 under 35 U.S.C. §103(a) as being unpatentable over Wang for the same reasons as those cited above for claim 36. However, claim 72 recites language similar to that recited in claim 36. For the reasons stated above with respect to claim 36, Wang also fails to teach or suggest claim 72.

In light of the forgoing remarks, Applicant respectfully requests the allowance of all pending claims 1-77.

Respectfully submitted,

COATS & BENNETT, P.L.L.C.

Dated: January 6, 2005

Stephen A. Herrera
Registration No.: 32,194

P.O. Box 5
Raleigh, NC 27602
Telephone: (919) 854-1844